Shiv Nadar University Chennai

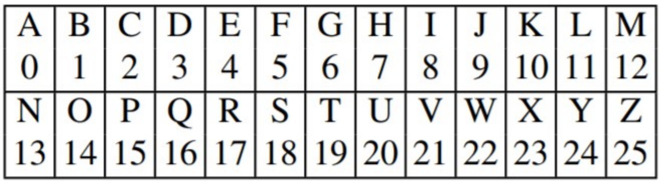
End Semester Examinations, 2022-2023 Even

Question Paper

Name of the Program: B.Tech. CSE (Cyber Security)		Semester: II
Course Code & Name: **CS1008 CLASSICAL CRYPTOGRAPHY**		
Regulation 2021		
Time: 3 Hours		Maximum: 100 Marks

Q.No		Questions	Marks	CO#	KL#
1	a	In asymmetric key cryptography, the private key is kept by __________. A) sender B) receiver C) sender and receiver D) all the connected devices to the network	1	CO2	KL1
	b	Which one of the following algorithm is not used in asymmetric-key cryptography? A) RSA algorithm B) Diffie-Hellman algorithm C) Electronic Code Book algorithm D) DSA algorithm	1	CO2	KL3
	c	In cryptography, the order of the letters in a message is rearranged by _______ A) Transposition ciphers B) Substitution ciphers C) Both Transposition ciphers and Substitution ciphers D) Quadratic ciphers	1	CO1	KL2
2	a	What is data encryption standard (DES)? A) Block cipher B) Stream cipher C) Bit cipher D) Byte cipher	1	CO4	KL2
	b	Which one of the following is a cryptographic protocol used to secure HTTP connection? A) Stream control transmission protocol (SCTP) B) Transport layer security (TLS) C) Explicit congestion notification (ECN) D) Resource reservation protocol	1	CO3	KL3
	c	Which of the following hash algorithm is not recommended? A) SHA2 B) SHA3 C) MD5 D) None of the above	1	CO4	KL1
3	a	How many bits SHA1 hash will have? A) 128 bits B) 160 bits	1	CO2	KL2

		C) 256 bits D) 512 bits			
	b	Which of the following options correctly defines the Brute force attack? A) Brutally forcing the user to share useful information like pins and passwords. B) Trying every possible key to decrypt the message. C) One entity pretends to be some other entity D) The message or information is modified before sending it to the receiver.	1	CO1	KL3
	c	Which of the following is true about digital signature. A) It provides integrity B) It provides authentication C) It provides integrity and authentication D) It provides confidentiality, integrity and authentication	1	CO2	KL6
4	a	Which of the following is the function of checksum? A) Block errors B) Add noise C) Detect errors D) All the above	1	CO4	KL4
	b	Stream Cipher converts the plain text into cipher text by taking 1 byte of plain text at a time. A) True B) False	1	CO2	KL2
	c	Which of the following is not an authentication service. A) Kerberos B) Digital Signature C) X.509 D) DNS	1	CO1	KL1
5	a	In Rail Fence Cipher, if the plain text 'cryptography' what will be the cipher text with 2 rails? A) ctarporpyygh B) cytgahrporpy C) cgroryytahpp D) carrpyghpoyt	1	CO3	KL3
	b	Which of the following is not a steganography tool? A) Xaio steganography B) OpenPuff C) ReaperExploit D) Steghide	1	CO4	KL4
	c	The main motive for using steganography is that hackers or other users can hide a secret message behind a _______________. A) Special file B) Ordinary file C) Program file D) Encrypted file	1	CO1	KL5

<table>
<tr><td>6</td><td>a</td><td>A _______________ is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic.
A) Server
B) Firewall
C) Router
D) None of the Above</td><td>1</td><td>CO3</td><td>KL6</td></tr>
<tr><td></td><td>b</td><td>Which statement is true regarding the GCD of three or more numbers?
A) It can only be calculated using the extended Euclidean algorithm.
B) It is always equal to the product of the three numbers.
C) It is the largest number that divides all three numbers without leaving a remainder.
D) It can only be calculated using prime factorization.</td><td>1</td><td>CO3</td><td>KL2</td></tr>
<tr><td></td><td>c</td><td>In Euclid's algorithm, if the two numbers being considered are 252 and 105, how many iterations are required to find their GCD?
A) 3
B) 4
C) 5
D) 6</td><td>1</td><td>CO2</td><td>KL1</td></tr>
<tr><td>7</td><td>a</td><td>The extended Euclidean algorithm is primarily used for solving which type of problems?
A) Linear equations
B) Quadratic equations
C) Diophantine equations
D) Polynomial equations</td><td>1</td><td>CO4</td><td>KL2</td></tr>
<tr><td></td><td>b</td><td>If the extended Euclidean algorithm is applied to find the modular inverse of a number modulo m, what condition must be satisfied for the modular inverse to exist?
A) The number and m must be coprime (relatively prime).
B) The number must be prime.
C) The number must be greater than m.
D) The number must be a perfect square.</td><td>1</td><td>CO1</td><td>KL3</td></tr>
<tr><td>8</td><td>a</td><td>What is Substitution Technique in cryptography?</td><td>2</td><td>CO3</td><td>KL3</td></tr>
<tr><td></td><td>b</td><td>Perform Caesar Cipher for the input ‘DHONI IS CAPTAIN COOL’ with offset of ‘+5’. What is the cipher text?
<table>
<tr><td>A
0</td><td>B
1</td><td>C
2</td><td>D
3</td><td>E
4</td><td>F
5</td><td>G
6</td><td>H
7</td><td>I
8</td><td>J
9</td><td>K
10</td><td>L
11</td><td>M
12</td></tr>
<tr><td>N
13</td><td>O
14</td><td>P
15</td><td>Q
16</td><td>R
17</td><td>S
18</td><td>T
19</td><td>U
20</td><td>V
21</td><td>W
22</td><td>X
23</td><td>Y
24</td><td>Z
25</td></tr>
</table></td><td>2</td><td>CO4</td><td>KL6</td></tr>
<tr><td></td><td>c</td><td>Write any four different points between Cryptography and Steganography.</td><td>2</td><td>CO2</td><td>KL1</td></tr>
<tr><td>9</td><td>a</td><td>What is Stream Cipher in cryptography?</td><td>2</td><td>CO1</td><td>KL3</td></tr>
<tr><td></td><td>b</td><td>What is an Intruder? What are categories of Intruders?</td><td>2</td><td>CO3</td><td>KL1</td></tr>
<tr><td></td><td>c</td><td>What is Man-in-the-middle attack? How to prevent being a victim of that?</td><td>2</td><td>CO2</td><td>KL4</td></tr>
<tr><td>10</td><td>a</td><td>What is ‘Non-Repudiation’ in cryptography and how it is achieved?</td><td>2</td><td>CO3</td><td>KL3</td></tr>
</table>

	b	What is the purpose of a key in cryptography, and how does it relate to the encryption and decryption processes?	2	CO1	KL2
	c	What is the purpose of a digital signature in cryptography, and how does it provide integrity and authenticity?	2	CO2	KL3
11	a	Explain the significance of unbreakable encryption cryptography.	2	CO4	KL1
12	a	Explain RSA algorithm, working of RSA & RSA disadvantages.	5	CO4	KL2
13	a	Explain DNS Spoofing and DNSSEC.	5	CO4	KL2
14	a	Explain Kerberos in detail.	5	CO3	KL2
15	a	Explain Intrusion Prevention System in detail.	5	CO2	KL3
16	a	Find the solution for the following system of congruence: X≡1(mod 2) X≡2(mod 3) X≡3(mod 5)	5	CO1	KL3
17	a	Alice wants to send a confidential message to Bob using a cryptographic system. She decides to encrypt the message using the RSA algorithm. Alice's RSA public key is (e, n) = (13, 253), and her RSA private key is (d, n) = (37, 253). However, before encrypting the message, Alice wants to ensure that it is not divisible by any small prime numbers to enhance the security of the encryption. To achieve this, Alice applies a modification to her message using the GCD (Greatest Common Divisor) operation. a) Explain how Alice can modify her message using the GCD operation to ensure it is not divisible by small prime numbers. b) Suppose Alice's original message is 212. Show the step-by-step process of modifying the message using the GCD operation to ensure it is not divisible by small prime numbers. c) Explain why modifying the message using the GCD operation enhances the security of the RSA encryption process.	5	CO1	KL6
18	a	Explain Block Cipher, its operation modes, advantages & disadvantages of each modes and applications of block cipher.	10	CO3	KL5
19	a	Explain of Certificate Authorities and Chain of Trust in details.	10	CO4	KL2
20	a	Suppose that p and q are distinct primes, a^p≡a (mod q) and a^q≡a (mod p), prove that a^pq≡a (mod pq).	10	CO1	KL1

KL – Bloom's Taxonomy Levels
(KL1: Remembering, KL2: Understanding, KL3: Applying, KL4: Analyzing, KL5: Evaluating, KL6: Creating)
CO – Course Outcomes
